

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

FILED
RB

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No:

1:10cv156
(LMB/JFA)

FILED UNDER SEAL

**APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY
TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft"), by counsel, pursuant to Federal Rule of Civil Procedure 65(b) and (c), the Computer Fraud and Abuse Act (18 U.S.C. §1030), the CAN-SPAM Act (15 U.S.C. §7704), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125 and the common law, respectfully moves the Court for an emergency *ex parte* temporary restraining order and order to show cause why a preliminary injunction should not issue. As discussed further in Microsoft's brief in support of this motion, Microsoft requests an order turning off 273 internet domains operated by the John Doe Defendants, which control a computer "botnet." The requested relief is necessary to halt the growth of the botnet which is causing irreparable injury to Microsoft, its customers and the public. Therefore, Microsoft respectfully requests that the Court grant this motion.

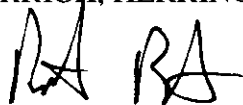
Microsoft further respectfully requests oral argument on this motion to be set for Monday, February 22, 2010.

1125

Dated: February 22, 2010.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP



PRESTON BURTON (Va. State Bar No. 30221)
REBECCA L. MROZ (Va. State Bar No. 77114)
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
pburton@orrick.com
bmroz@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)
JACOB M. HEATH (*pro hac vice* application pending)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com

Attorneys for Plaintiff Microsoft Corp.

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No:

FILED UNDER SEAL

**BRIEF IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION
FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER
AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I. INTRODUCTION

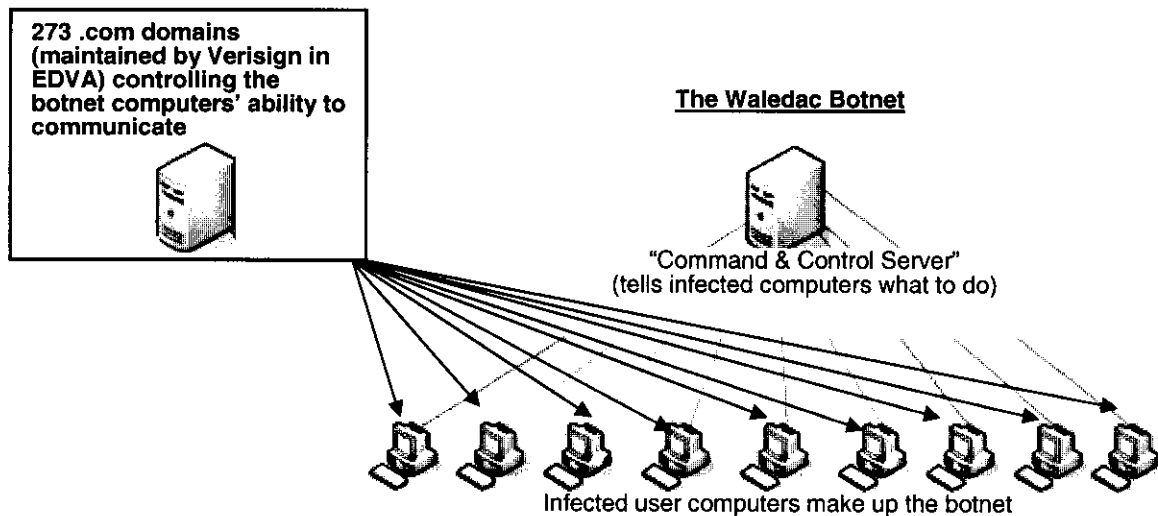
Microsoft Corp. ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and preliminary injunction to halt the growth of a computer "botnet" causing extreme and irreparable injury to Microsoft, its customers and the public. Microsoft specifically seeks *ex parte* relief because notice to John Doe Defendants 1-27 ("Doe Defendants") would render the requested relief fruitless and result in destruction of evidence. A botnet is a network of compromised user computers under the control of criminals, used to carry out harmful conduct. Doe Defendants control the "Waledac" botnet, which is comprised of over 390,000 compromised user computers and are likely part of a broader organization of malicious actors. Twenty six Doe Defendants provided domain contact information in China and one Doe Defendant provided U.S. contact information.

Approximately every 18 days, the Waledac botnet is sending over 651 million unsolicited harmful "spam" emails to Microsoft Hotmail email users alone. The scale of this attack and the

resulting irreparable harm are overwhelming to Microsoft and its customers, both placing incredible burden on the company's technical resources and causing long-term injury to Microsoft's goodwill and customer relationships. This situation is an emergency, warranting the relief sought in this motion to temporarily disable the internet domains that control and grow the botnet and compound this injury. If those internet domains are not halted during the pendency of this action, Microsoft's business, goodwill and relationships with its customers will be irreparably harmed as this threat grows and continues. There is also great public harm if emergency relief is not granted, as the Waledac botnet, conservatively, can disseminate an estimated 1.5 billion unsolicited and harmful spam emails per day, delivers malicious computer code, steals personal information and controls users' computers without their authorization.

Doe Defendants have registered and are using 273 ".com" internet domains at issue in this motion *solely* to control and grow the Waledac botnet. There is no legitimate activity at these domains. The 273 domains are maintained by the ".com" domain registry, Verisign, Inc., in the Eastern District of Virginia. Microsoft requests an order that Verisign turn off these 273 domains, thus halting the botnet's expansion and the resulting irreparable injury.

The following is a general representation of the relationship of the 273 domains at issue in this motion and the Waledac botnet:



The botnet is estimated to contain approximately 390,000 compromised user computers and the 273 domains at issue in this motion enable that number to grow. By infecting these computers the controller of the botnet, without authorization, intruded upon Microsoft's licensed operating system and computers of Microsoft's customers. Infected computers are used to carry out illicit activities, in particular sending billions of unsolicited, deceptive and illegal spam emails, collecting personal information such as email addresses, delivering malicious code and other actions to grow the botnet. The performance of compromised user computers is severely and negatively impacted by these activities. These are criminal activities, including violations of statutes such as the Computer Fraud & Abuse Act and the CAN-SPAM Act, which also provide a private right of action to companies like Microsoft.

Microsoft's reputation, brand and goodwill are injured because the Waledac botnet directs an enormous amount of harmful spam emails per day to Microsoft Hotmail® accounts. Microsoft and its customers are improperly forced to bear this burden. Microsoft's customers are led to incorrectly believe that Microsoft, the provider of Hotmail, is the cause of harmful spam email. Microsoft is injured because users of infected computers incorrectly believe that Microsoft, the maker of the popular Windows® operating system installed on many computers, is the source of problems caused by the botnet. Microsoft has receives approximately 3000 complaints caused by the botnet and must expend substantial resources dealing with the injury and confusion. The injury also extends far beyond Microsoft to all computer users, each of whom is a target of the botnet and whose computers may be compromised. Thus, there is a strong public interest in obtaining relief.

The injury caused by the Waledac botnet is severe, irreparable and ongoing. The scale of the botnet and its operations are overwhelming. Further, the botnet uses a sophisticated architecture that is resistant to technical mitigation efforts. Absent a TRO and preliminary

injunction, the injury will continue unabated, irreparably harming Microsoft's reputation, brand and products, harming its relationships with customers, and harming the public. Microsoft requests an order that immediately (1) turns off the 273 domains controlling the botnet at the .com "top level domain" registry (Verisign) and at the domain name registrars and (2) places the domains in escrow with Verisign, so that the injury is not further compounded and evidence of misconduct is preserved.

The only way to achieve relief is by granting an *ex parte* TRO turning off the harmful domains, immediately after which Microsoft will effect notice and service on the Doe Defendants, and sealing the proceedings for three business days. Based on Microsoft's and third parties' prior experience, there is an overwhelming risk that if notice is given before temporary relief is granted, Doe Defendants will immediately move the botnet to new, unidentified locations, allowing Doe Defendants to continue their misconduct and resultant injury with impunity. During prior efforts where parties in control of botnets were notified in advance and offending domains were not turned off at the domain registry, this was precisely the result. The Waledac botnet has been designed with features to effect exactly this type of evasion.

Thus, unless *ex parte* relief is granted, the severe and irreparable injury caused by the Waledac botnet will be compounded and evidence of misconduct will be moved or destroyed. By granting the requested relief, the Court would preserve the status quo, contain the damage and preserve necessary evidence. Granting the requested relief will turn off domains having the sole purpose of supporting the botnet and its malicious activity. There is no legitimate activity associated with such domains. The balance of harms weighs heavily in favor of granting a TRO and preliminary injunction.

Microsoft is prepared to engage in robust efforts to provide notice of the preliminary injunction hearing and to effect service of process on the Doe Defendants immediately upon the

Court's issuance of the requested relief. To ensure prompt effective notice, Microsoft requests that the Court permit it to provide notice of the preliminary injunction hearing and service of the complaint through both formal and alternative means as part of the relief sought herein.

II. STATEMENT OF FACTS

A. The Waledac Botnet

A "botnet" is a collection of individual computers, each running software that allows communication among those computers and includes computers providing control instructions to the rest of the botnet computers. (Declaration of David Dittrich ("Dittrich Decl."), ¶¶ 3-6) This case involves a botnet known as the "Waledac" botnet. The Waledac botnet is made up of computers belonging to individual users who have unknowingly downloaded and been infected by software that renders their computers part of the botnet. (Dittrich Decl., ¶¶ 7, 24-26); Declaration of T.J. Campana ("Campana Decl."), ¶¶ 13-15, Exs. 2-3; Declaration of Dean Turner ("Turner Decl."), ¶¶ 16-22) For example, a user may inadvertently interact with a malicious website advertisement, click on a malicious email attachment or download a fraudulent software product, causing their computer to become infected and part of the botnet. (*Id.*) The spread of the Waledac botnet in this way is not related to any vulnerability in Microsoft's systems, but is instead achieved by misleading unwitting users into taking steps that result in the infection of their machines. (Campana Decl., ¶ 13)

Once part of the botnet, the user's computer is under control of the parties controlling the botnet. (Dittrich Decl., ¶¶ 7, 24-25; Campana Decl., ¶¶ 24-31) The parties controlling the botnet steal personal information, such as email addresses from the user's computer. (Dittrich Decl., ¶ 8, Campana Decl., ¶ 44) The parties controlling the botnet can cause the user's computer to send billions of bulk, unsolicited, harmful "spam" emails every day, deliver malicious software to infect other computers or otherwise use it to carry out fraud, computer intrusions or other

malicious and illegal conduct. (Dittrich Decl., ¶¶ 8-14, 24-32; Campana Decl., ¶¶ 4, 19-44).

Much of this activity is criminal conduct. (Dittrich Decl., ¶¶ 8-14, Exs. B-E; Ramsey Decl., Exs. N-O)

The Waledac botnet is created and controlled by a sophisticated organization carrying out unlawful conduct. (Dittrich Decl., ¶¶ 3-15; Turner Decl., ¶¶ 1-15) It is believed that the botnet is used both to conduct activities which directly generates profits, such as sending unsolicited, harmful spam email in order to improperly generate advertising revenue. The parties in control of the botnet also sell capacity on the botnet to others who carry out such activities. (Dittrich Decl., ¶ 9, Exs. B-E)

B. The Structure, Operation And Illegal Activity of the Waledac Botnet

Microsoft has recently investigated the structure of the Waledac botnet. (Campana Decl., ¶ 2; Dittrich Decl., ¶¶ 15-23) The botnet is made up of a tiered architecture. Infected computers in some tiers are used to carry out spam email attacks. Infected computers in other tiers are simply used to relay and “proxy” communications between computers in the botnet and the outside world, to obfuscate the source of communications. At the highest level of the botnet is one or more “command and control” computers, from which the parties controlling the botnet deliver instructions and code directing the botnet to carry out various illegal activities. (See Dittrich Decl., ¶¶ 15-23, Ex. G; Campana Decl., ¶¶ 3-18; Turner Decl., ¶¶ 23-33)

C. The 273 Domains At Issue In This Motion Control The Waledac Botnet’s Ability To Communicate And Grow And The Domains Have No Legitimate Purpose

Critical to the Waledac botnet are 273 domains, listed at Appendix 1 to the Campana Declaration, filed herewith, and which are the subject of this motion. (Campana Decl., Ex. 1) These 273 domains continuously control the ability of the computers that make up the Waledac botnet to communicate with each other and to grow the botnet. (Campana Decl., ¶¶ 10-18;

Dittrich Decl., ¶¶ 16-23, 33-34) In particular, if a given computer in the Waledac botnet is unable for some reason to continue perpetuating the growth of the botnet, sending malicious commands to other computers or sending spam emails from the botnet, the computer will automatically check these 273 domains for instructions about how to continue carrying out these activities. (*Id.*) Additionally, links to the 273 domains may be included in unsolicited, spam email sent out by the botnet, with the purpose of spreading the botnet. (*Id.*) These emails usually mislead the recipient by appearing to link to a news story or e-card. (*Id.*) When the victim opens the link in the email, the botnet may deliver software that infects the victim's computer and makes it part of the Waledac botnet. (*Id.*)

These 273 domains have no legitimate purpose. (Campana Decl., ¶17; Dittrich Decl., ¶16) Rather, the domains are controlled by the criminals behind the botnet. The domains' sole purpose is to await requests from botnet computers and instruct them on how to continue communicating with each other and to infect new user computers. (*Id.*) In this way, the domains support, propagate and grow the botnet and enable malicious activities carried out through it.

D. The Waledac Botnet Irreparably Harms Microsoft, Its Customers And The Public

The Waledac botnet has caused and continues to cause irreparable injury to Microsoft, its customers and the public. (Campana Decl., ¶¶ 19-44; Dittrich Decl., ¶¶ 24-32)

Microsoft and its customers are injured when the Waledac botnet software is maliciously introduced onto users' computers making them part of the botnet.¹ (Campana Decl., ¶¶ 24-31; Dittrich Decl. ¶¶ 24-27) These acts constitute an unauthorized intrusion into the Microsoft

¹ The malicious software that perpetuates the Waledac botnet is known by various names in the Internet security community, including: Win32/Iksmas.worm.390656 (AhnLab), Trojan.Waledac.F (BitDefender), Win32/Waledac.D (CA), Email-Worm.Win32.Iksmas.y (Kaspersky), W32/Waledac.gen (McAfee), Trj/MailStealer.F (Panda), W32/Waled-F (Sophos), W32.Waledac (Symantec), Trojan.Waledac.Gen (VirusBuster). (Campana Decl., ¶ 24)

Windows® operating system in which Microsoft retains a possessory interest. (Campana Decl., ¶¶ 24-31, Exs. 6-7; Dittrich Decl. ¶¶ 24-27) The Waledac botnet specifically targets the Windows® operating system. (Campana Decl., ¶¶ 25-27) For example, it writes particular entries to the registry of the Windows® operating system, without the consent of Microsoft or its customers. (*Id.*) Similarly, the botnet installs and runs fake “anti-virus” software under the misleading name “MS Antispyware 2009,” which is designed to mislead consumers into installing the software. (Campana Decl., ¶¶ 42-43, Ex. 2 at p. 30; Dittrich Decl., ¶¶ 24, 31-32) The unauthorized software causes injury by degrading the performance of the user’s computer and misleading Microsoft’s customers. (*Id.*)

Microsoft and its customers are injured when the Waledac botnet causes customers’ computers to send billions of harmful spam emails to Microsoft’s Hotmail® email service. Microsoft recently conducted an analysis of spam email originating from the Waledac botnet and learned that in a brief 18 day period the botnet attempted to send over 651 million emails to Microsoft’s Hotmail users and was ultimately able to cause between 700,000 and 2.5 million such emails per day to reach those users in the same period. (Campana Decl., ¶¶ 32-41) Security researchers examining the Waledac botnet conservatively estimate that it is capable of sending 1.5 billion harmful spam emails per day (Campana Decl., ¶ 32, Ex. 4 at p. 7; Dittrich Decl., ¶¶ 28-30). The following chart sets forth the results of Microsoft’s recent research:

| Date | Total Waledac IP Addresses Sending Harmful Spam Email | Total Attempted Email Connections To Hotmail Addresses From Waledac IP Addresses | Total Emails From Waledac IP Addresses That Reached Hotmail Users |
|------|--|---|---|
| 12/3 | 11,924 | 40,467,232 | 1,204,481 |
| 12/4 | 18,626 | 22,174,273 | 714,120 |
| 12/5 | 17,103 | 28,540,548 | 725,559 |
| 12/6 | 22,265 | 52,346,544 | 1,244,063 |
| 12/7 | 27,659 | 32,194,622 | 1,419,413 |
| 12/8 | 29,221 | 60,280,704 | 1,673,738 |
| 12/9 | 27,805 | 36,128,630 | 1,440,420 |

| | | | |
|--------------|----------------|--------------------|-------------------|
| 12/10 | 23,684 | 55,382,525 | 1,458,291 |
| 12/11 | 19,180 | 29,803,721 | 848,750 |
| 12/12 | 15,822 | 61,596,946 | 910,474 |
| 12/13 | 17,630 | 37,440,063 | 927,230 |
| 12/14 | 7,345 | 17,553,168 | 989,909 |
| 12/15 | 17,765 | 22,765,729 | 1,279,526 |
| 12/16 | 17,010 | 43,772,091 | 1,331,391 |
| 12/17 | 17,303 | 30,364,480 | 1,170,048 |
| 12/18 | 16,301 | 19,684,138 | 1,053,943 |
| 12/19 | 14,923 | 19,473,710 | 889,370 |
| 12/20 | 19,225 | 24,173,454 | 1,987,252 |
| 12/21 | 15,682 | 16,983,712 | 2,535,731 |
| Total | 179,485 | 651,126,290 | 23,803,709 |

Microsoft is further injured when such email is falsely made to appear to originate from Microsoft's Hotmail® email service. (Campana Decl., ¶ 37) Further, Microsoft and its customers are injured when the Waledac botnet collects and transmits personal information, including personal email address information, from users' computers. (Campana Decl., ¶ 44; Dittrich Decl., ¶¶ 8, 24)

Microsoft and its reputation, brand and goodwill are injured because users of compromised computers incorrectly believe that Microsoft is the source of computer problems caused by the botnet. (Campana Decl., ¶¶ 19-31) Microsoft is similarly injured because the botnet directs an extraordinary amount of spam email to users of Microsoft's email services and causes spam emails to appear to originate from Microsoft. Microsoft and its customers must bear this extraordinary burden and customers are incorrectly led to believe that Microsoft is to blame for the spam email. (*Id.*, ¶¶ 19-23, 32-41) Microsoft receives a large volume of customer support requests caused by the Waledac botnet and must expend substantial resources dealing with the injury and confusion. (*Id.*, ¶¶ 21)

Microsoft's customers leave Microsoft because of the Waledac botnet and there are significant challenges to getting them to return, given switching costs and the perceived risk of

returning (even though, in fact, the botnet threatens users of all platforms). (Campana Decl., ¶¶ 19-23) For this reason, the harm to Microsoft is irreparable. Once customers' computers are infected and become part of the botnet, they are unaware of that fact and may not have the technical resources to solve the problem, allowing their computers to be misused indefinitely. Thus extrajudicial, technical attempts to remedy the problem alone are insufficient and the injury caused to customers continues. (*Id.*, ¶¶ 21-22) Further, the injury caused by the Waledac botnet extends far beyond Microsoft to other consumers and providers of email services and all computer users, each of whom is at risk. (Dittrich Decl., ¶¶ 3-14, Exs. B-F; Turner Decl., ¶¶ 1-33; Declaration of André M. DiMino, ¶¶ 1-11)

E. Turning Off The 273 Domains Controlling The Waledac Botnet Is Necessary To Prevent The Irreparable Injury To Microsoft, Its Customers And The Public

The Waledac botnet is designed to resist technical mitigation efforts, eliminating viable technical means to curb the injury short of the relief requested in this motion. (Campana Decl., ¶¶ 8-9; Dittrich Decl., ¶¶ 17-23) Similarly, piecemeal requests to turn off the domains or informal dispute resolution are insufficient as once notified, will result in movement and hiding of the botnet. (Campana Decl., ¶¶ 45-47; Dittrich Decl., ¶¶ 33-35) Accordingly, to effect a TRO and preliminary injunction that will temporarily halt the irreparable injury, it is necessary that the order immediately:

- (1) turn off the resolution of the 273 domains used to control the botnet at Verisign—the “top level domain” registry for .com domains—and also at the individual domain name registrars, and
- (2) place the domains in escrow with Verisign, so that the injury is not further compounded and evidence of misconduct can be preserved.

(*Id.*) This is the only possible means to stop the irreparable harm pending resolution of this case. (*Id.*)

F. The Botnet Will Be Moved And Concealed And Evidence Destroyed If Notice Of The Requested Relief Is Given In Advance.

The only way to achieve relief from the irreparable injury is by granting *ex parte* relief turning off the domains. To do otherwise would render the relief fruitless and the harm to Microsoft would continue. This is because if notice is given or if the domains are turned off in piecemeal fashion, there is an overwhelming risk that the botnet and the domains controlling it will be moved to new, unidentified locations, allowing them to continue the injury. (Campana Decl., ¶¶ 45-47; Dittrich Decl., ¶¶ 33-35) This was precisely the result in prior efforts to obtain relief from damage caused by botnets, where the botnet controllers were notified in advance or informal attempts were made to turn off domains at the registrars, one at a time.² (*Id.*) For example, the criminal indictment of one botnet controller describes that when the botnet controller was informally told by his Internet Service Provider that his servers would be shut down, he made a “change to redirect the bots in that channel to navigate to a different adware server, one... that he controlled, or to which he had access...,” allowing the malicious botnet operations to continue. (Ramsey Decl., Ex. N at pg. 39, ¶227) The same would occur here if notice were given to the similarly situated botnet controllers in advance of the requested emergency relief.

Thus, unless *ex parte* relief is granted, injury caused by the botnet will be compounded and evidence of misconduct and the botnet’s operation will be moved or destroyed. By granting this motion, the irreparable injury will be contained and the evidence preserved. Further, the requested relief will not affect any legitimate interests of any party. Rather, the requested relief will turn off domains which have the *sole* purpose of supporting the botnet.

III. ARGUMENT

Microsoft seeks a TRO and preliminary injunction, pursuant to Federal Rule of Civil

² It is for this reason that ICANN’s dispute resolution processes regarding domains is not a viable means to suspend the irreparable injury caused by defendants’ 273 botnet domains.

Procedure 65, to prevent compounding of the harm and to ensure that evidence of misconduct is preserved during the pendency of this case. In determining whether to grant preliminary equitable relief, the Fourth Circuit requires a showing that: (1) the moving party is likely to succeed on the merits; (2) the moving party is likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities to tip in the moving party's favor; and (4) an injunction is in the public interest. See *Winter v. NRDC, Inc.*, 129 S. Ct. 365, 374-376 (2008); *Real Truth About Obama, Inc. v. Federal Election Com'n.*, 575 F.3d 342, 346-47 (4th Cir. 2009) (adopting *Winter* test).

Microsoft is very likely to succeed on the merits. The Waledac botnet's sending of hundreds of millions of spam emails to Microsoft's services and customers, unlawful intrusion and collection of personal information and deceptive use of Microsoft's brand violates the federal Computer Fraud & Abuse Act, CAN-SPAM Act and Lanham Act and further constitutes deceptive, misleading and tortious conduct in violation of state law. Microsoft and its customers will be irreparably harmed if the botnet continues to operate through the 273 domains at issue in this motion. By contrast, the *only* conduct carried out on the domains is dissemination of malicious code and control of a botnet, which is unauthorized in itself and is used to carry out further illegal conduct. Thus, there is no harm to the Doe Defendants if the TRO and preliminary injunction should issue. Additionally, the public interest weighs very heavily in favor of relief because the same harm the botnet is causing to Microsoft and its customers is also imposed on many other U.S. computer users and companies as well.

A. Irreparable Harm Will Result If A TRO And Preliminary Injunction Are Not Granted

Continued operation of the Waledac botnet irreparably harms Microsoft, its customers and the public. There would be no monetary remedy that can make Microsoft or its customers whole if the botnet were permitted to continue operating and expanding. In one of the only cases

specifically addressing botnets, a federal court very recently found that “immediate and irreparable harm” will result to consumers from “botnet command and control servers, spyware, viruses, trojans, and phishing-related sites; and configuring, deploying and operating botnets,” and issued an *ex parte* TRO and preliminary injunction on that basis. *See FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.) at Dkt. 12, pg. 2 (June 2, 2009 *Ex Parte* Temporary Restraining Order and Order to Show Cause) and Dkt. 37, pgs. 2-3 (June 15, 2009 Preliminary Injunction), submitted herewith at Ramsey Decl., Exs. L and M.

The same type of irreparable injury is currently occurring to Microsoft and its customers. Thus, entry of an *ex parte* TRO and Order to Show Cause why a preliminary injunction should not issue is warranted. First, Microsoft is irreparably injured because problems of spam email and system performance caused by the botnet are improperly attributed to Microsoft. Microsoft’s customers may migrate to other platforms, products or services in the belief that Microsoft is the cause of the problems. (Campana Decl., ¶¶ 19-23). Once such change is effected, given the costs of switching platforms and the uncertainty caused by the botnet in the first place, there is a very high risk that those customers will not return to Microsoft. As the botnet continues to grow and expand, this harm is compounded. This type of brand related injury and customer harm is most certainly irreparable and is precisely why the relief requested in this motion should be granted. *See Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994) (“when the failure to grant preliminary relief creates the possibility of permanent loss of customers to a competitor or the loss of goodwill, the irreparable injury prong is satisfied”)

Further, if the requested relief were not granted, the computers of Microsoft’s customers will continue to be infected and the botnet will grow. This injury is irreparable because customers without the technical resources to remedy the problem will not be able to do so. They

will be under constant threat of unauthorized intrusion and abuse once their computers are infected and made part of the botnet. Long term injury of this type constitutes irreparable harm warranting the entry of the requested relief. *See Arminius Schleifmittel GmbH v. Design Indus., Inc.*, 2007 U.S. Dist. LEXIS 10847, *22 (M.D.N.C. 2007) (irreparable harm where defendant's actions "will have significant and continuous long-term effects").

B. Doe Defendants Will Suffer No Harm By Maintaining The Status Quo

Doe Defendants will suffer *no harm* if a TRO and preliminary injunction are issued, because it will do no more than preserve the status quo. That is, by turning off the 273 domains at the domain registry and registrars and ordering those domains be held in escrow while this dispute is pending, no additional computers will be infected by the Waledac botnet during that time and evidence of the botnet's structure and illegal conduct will be preserved. Doe Defendants will suffer no harm if a TRO and preliminary injunction are issued because the 273 domains' sole purpose is to carry out illegal activity. (Campana Decl., ¶ 17) There is no risk that any legitimate activity will be affected. Thus, Doe Defendants will suffer no harm through preservation of the status quo pending adjudication of the issues in dispute. *See Allegra Network LLC v. Reeder*, 2009 U.S. Dist. LEXIS 103688, *10 (E.D. Va. 2009) (preliminary injunction issued where there was no evidence that Doe Defendants would suffer irreparable harm from not being able to carry out enjoined activities).

If, on the other hand, a TRO and preliminary injunction do not issue, the injury caused by the Waledac botnet cannot be contained. The botnet already includes 390,000 compromised user computers, sending on the order of 651 million spam emails to Hotmail users in less than a month and capable of sending 1.5 billion spam emails per day. New users are infected each day, exponentially increasing the capabilities to carry out illegal conduct, compounding the injury to Microsoft, its customers and the public. Simply put, maintaining the status quo by turning off

the botnet domains will not affect any legitimate rights of the Doe Defendants, yet allowing the botnet to grow and to permit continued abuse to Microsoft, its customers and the public while this action is adjudicated poses grave danger to many legitimate interests.

C. The Public Interest Will Be Served By Issuance Of A TRO And Preliminary Injunction

It is exceedingly important to recognize the degree to which the TRO and preliminary injunction protects the public interest beyond Microsoft and its own customers. Indeed, every consumer with access to an email platform and the Internet is at risk of being irreparably injured by the Waledac botnet. Similarly, every company providing email services and websites are at risk of having their systems misused to perpetuate the botnet. Further, the spam email sent by the Waledac botnet pushes fake and potentially dangerous pharmaceuticals, pirated and counterfeit goods and promotes fraudulent schemes that can injure consumers. (Campana Decl., ¶¶ 38-41, Ex. 8) There is an overwhelming public interest in preserving the status quo and halting the growth of the Waledac botnet while Microsoft proceeds with its claims. This Court has emphasized in a similar case “a strong public interest in granting preliminary injunctive relief” and noted that “[t]his Court has an obligation to enjoin any alleged computer hackers from continuing to attack and steal [plaintiff’s] proprietary information.” *Physicians Interactive v. Lathian Systems, Inc.*, 2003 U.S. Dist. LEXIS 22868, *30 (E.D. Va. 2003) (granting TRO and preliminary injunction where defendant hacked into a computer and stole confidential information). More specifically, it was recently found that “immediate and irreparable harm” will result to the welfare of consumers from “botnet command and control servers” and the malicious conduct carried out through botnets. *See Federal Trade Commission v. Pricewert LLC et al.* at pg. 2 (Ramsey Decl. Ex. L (granting *ex parte* TRO)). Similarly, here a TRO and preliminary injunction will preserve and protect this important public interest. No such protection will be afforded if preliminary relief is denied and, in that event, the criminals

controlling the botnet will be able to continue their activities with impunity.

D. Microsoft Is Very Likely To Succeed On The Merits Of Its Claims

Microsoft is very likely to succeed on the merits of its claims, thus its request for preliminary relief should be granted. The Complaint sets forth the following statutory and common law claims: (1) violations of Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) violations of the CAN-SPAM Act (15 U.S.C. § 7704), (3) violations of the Electronic Communications Privacy Act (18 U.S.C. § 2701), (4) false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)), (5) trademark dilution under the Lanham Act (15 U.S.C. 1125(c)), (6) computer trespass, (7) unjust enrichment, and (8) conversion.

1. Computer Fraud And Abuse Act

The Computer Fraud and Abuse Act (“CFAA”) penalizes, among other things, a party who:

- “intentionally accesses a protected computer³ without authorization, and as a result of such conduct, causes damage.” 18 U.S.C. § 1030(a)(5)(C), or;
- “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer.” (18 U.S.C. § 1030(a)(2)(C)), or;
- “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.” (18 U.S.C. § 1030(a)(5)(A)).

The parties controlling the botnet intentionally access and send malicious code to Microsoft’s and its customers’ protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet. The evidence submitted in support of this motion demonstrates that Microsoft and its customers are damaged by this intrusion. Performance of Microsoft’s and its customers’ computers is degraded due to

³ A “protected computer” is a computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States.”

the unauthorized intrusion, running of malicious code, collecting of personal information and carrying out of malicious conduct. Microsoft's Hotmail servers are burdened by the sending of an enormous amount of spam email to Microsoft's Hotmail accounts.

This is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See e.g. Physicians Interactive v. Lathian Systems, Inc.*, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA).⁴ Indeed, some courts have aptly observed that the CFAA was targeted at "computer hackers (e.g., electronic trespassers)." *State Analysis, Inc. v. American Fin. Svcs. Assoc.*, 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (citation omitted).

Further, spam emails sent by the Waledac botnet to Hotmail users, burdening Microsoft's servers supporting that service and interfering with its goodwill, are actionable under the statute. *See e.g. America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (defendant's spamming in violation of plaintiff's terms of service violated CFAA); *Hotmail Corp. v. Van\$ Money Pie Inc.*, 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (granting preliminary injunction under CFAA where defendant sent spam email to Hotmail subscribers without their authorization). Similarly, here Microsoft is likely to succeed on the merits of its Computer Fraud & Abuse Act claim against the unlawful intrusion, collection of email addresses and other personal information, spam email and similar misconduct carried out by the botnet.

18 U.S.C. § 1030(e)(2)(B).

⁴ Indeed, recent years botnet operators who disseminate code that intrudes upon user computers, collects personal information and causes injury have been indicted and convicted criminally under the Computer Fraud & Abuse Act. *See Ramsey Decl., Exs. N (Indictment of Jeanson*

2. CAN-SPAM Act

The CAN-SPAM Act prohibits, among other acts, initiation of a transmission of a commercial electronic mail message “that contains, or is accompanied by, header information that is materially false or materially misleading.” 15 U.S.C. § 7704(a)(1). Here, the Waledac botnet automatically sends emails containing false “header” information (i.e. originating sender, IP address, etc.) making the emails appear to originate from user computers, false Hotmail addresses or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. This is precisely what CAN-SPAM prohibits. *See Aitken v. Communs. Workers of Am.*, 496 F. Supp. 2d 653, 667 (E.D. Va. 2007) (inaccurate “from” line and header information may violate CAN-SPAM). Thus, Microsoft is likely to succeed on the merits of its CAN-SPAM Act claim.

3. Electronic Communications Privacy Act

The Electronic Communications Privacy Act prohibits “intentionally access[ing] without authorization a facility through which electronic communications are provided” or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft’s servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. The Waledac botnet software, installed without authorization on infected computers, searches files such as emails and other files and steals personal email addresses and other information from those sources. Once harvested, these stolen email addresses become targets for spam email or are used for other malicious purposes. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Global Policy Partners, LLC*, 2009 U.S. Dist.

James Ancheta), O (Sentencing of Jeanson James Ancheta).

LEXIS 112472, *8-13 (E.D. Va. 2009) (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc.*, 621 F. Supp. 2d at 317-318 (access of data on a computer without authorization actionable under ECPA). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

4. False Designation Of Origin And Trademark Dilution

The Lanham Act prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which:

is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a). The Waledac botnet misleadingly and falsely causes the famous and distinctive Microsoft® and Windows® trademarks to be associated with malicious conduct carried out on users' computers through improper use of Microsoft's Windows operating system. Similarly, the Waledac botnet misleadingly and falsely causes the famous and distinctive Hotmail® trademark to be the purported "source" of spam email and causes users of Hotmail to receive spam email. Further, the Waledac botnet misleadingly delivers fake and malicious antivirus software, misleadingly named "MS Antispyware 2009." This conduct causes confusion and mistake as to Microsoft's affiliation with such misconduct and creates the false impression that Microsoft is the origin, when it is not. This activity is a clear violation of Lanham Act § 1125(a), thus Microsoft is likely to succeed on the merits. *See e.g. America Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (spam email with purported "from" addresses including plaintiff's trademarks constituted false designation of origin.)

The Lanham Act also provides that the owner of a famous, distinctive mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark..." 15 U.S.C. §

1125(c). Here, the Waledac botnet's misuse of Microsoft's famous marks in connection with malicious conduct aimed at Microsoft's customers and the public dilutes these famous marks by tarnishment and by blurring of consumer associations with the marks. Again, this is a clear violation of Lanham Act § 1125(c), and Microsoft is likely to succeed on the merits. *See e.g. America Online*, 24 F. Supp. 2d at 552 (spam email with purported "from" addresses including plaintiff's trademarks constituted dilution).

5. Trespass To Chattels And Conversion

A trespass to chattels occurs "when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization," and "if the chattel is impaired as to its condition, quality, or value." *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451-452 (E.D. Va. 1998); *AOL v. IMS*, 24 F. Supp. 2d 548 (citing *Vines v. Branch*, 244 Va. 185, 418 S.E. 2d 890, 894 (1992)) (trespass to chattels actionable in Virginia); *see also Barr v. City of Roslyn*, 2010 U.S. Dist. LEXIS 5541, *6-7 (E.D. Wash. 2010) (same). Similarly, "[a] person is liable for conversion for the wrongful exercise or assumption of authority over another's goods, depriving the owner of their possession, or any act of dominion wrongfully exerted over property in denial of, or inconsistent with, the owner's rights." *James River Mgmt. Co. v. Kehoe*, 2009 U.S. Dist. LEXIS 107847, *22-23 (E.D. Va. 2009); *Barr*, 2010 U.S. Dist. LEXIS 5541 at *6-7 (under Washington law "conversion is the act of willfully interfering with any personal property without lawful justification, which causes the person entitled to possession to be deprived of that possession")

The unauthorized downloading of software and control over Microsoft's licensed Windows operating system software and computers of customers interferes with and causes injury to the value of those properties. Thus, this conduct is an illegal trespass and also constitutes conversion. *See Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868

(E.D. Va. 2003) (granting TRO and preliminary injunction where defendant hacked computers and obtained proprietary information holding “there is a likelihood that the two alleged attacks that [Plaintiff] traced to Defendants were designed to intermeddle with personal property in the rightful possession of Plaintiff.”); *State v. Riley*, 121 Wn. 2d 22, 32 (Wash. 1993) (affirming conviction for “computer trespass” under Washington law for defendant’s “hacking activity”); *Combined Ins. Co. v. Wiest*, 578 F. Supp. 2d 822, 835 (W.D. Va. 2008) (conversion of “an electronic version of [a document]”); *In re Marriage of Langham*, 153 Wn.2d 553, 566 (Wash. 2005) (conversion of intangible property).

Likewise, unauthorized intrusion into Microsoft’s servers providing the Hotmail service, by sending vast quantities of spam email, injures Microsoft’s property and constitutes a trespass. *See e.g. America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (senders of spam e-mail committed trespass when they “caused contact with [plaintiff’s] computer network ... and ... injured [plaintiff’s] business goodwill and diminished the value of its possessory interest in its computer network.”); *accord State v. Heckel*, 143 Wn. 2d 824, 834 (Wash. 2001) (spam email burdens possessory interest of computers, citing *AOL v. IMS*); *E.I. Dupont De Nemours & Co. v. Kolon Indus.*, 2009 U.S. Dist. LEXIS 76795, *25-26 (E.D. Va. 2009) (claim for conversion “based exclusively on the transfer of copies of electronic information”; noting that “Virginia courts have ... demonstrated a distinct willingness to expand the scope of the doctrine of conversion in light of advancing technology.”)

6. Unjust Enrichment

The elements of a claim of unjust enrichment are (1) the plaintiff’s conferring of a benefit on the defendant, (2) the defendant’s knowledge of the conferring of the benefit, and (3) the defendant’s acceptance or retention of the benefit under circumstances that “render it inequitable for the defendant to retain the benefit without paying for its value.” *Nossen v. Hoy*, 750 F.Supp.

740, 744-45 (E.D.Va. 1990) (Virginia law); *Ballie Commc'ns Ltd. v. Trend Bus. Sys. Inc.*, 61 Wn.App. 151, 160, 810 P.2d 12 (1991) (same, under Washington law). Here, without authorization, the parties controlling the botnet have taken the benefit of Microsoft's servers, networks and email services, its licensed Windows operating system software and the computers of Microsoft's customers. They have done so by improperly infecting these computers, collecting personal information and causing them to send and receive spam email. Thus, it is certainly inequitable for the parties controlling the botnet to retain this benefit. Microsoft is likely to succeed on the merits.

E. Only The *Ex Parte* Relief Requested In This Motion Can Halt The Irreparable Injury

Absent a TRO granting the relief requested herein, the injury to Microsoft, its customers and the public, will continue, unabated, irreparably harming Microsoft's reputation, brand and goodwill, Microsoft's customers and the public. The TRO must be granted *ex parte* in order for relief to be effective at all and there are extraordinary circumstances warranting such relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); see *Granny Goose Foods, Inc. v. Teamsters*, 415 U.S. 423, 438-39, 94 S.Ct. 1113 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances...."); *Hoechst Diafoil Co. v. Nan Ya Plastics Corp.*, 174 F.3d 411, 422 (4th Cir. 1999) ("temporary restraining orders may be issued without full notice, even, under certain circumstances, *ex parte*").

1. If Notice Is Given, The Botnet Will Be Moved And Concealed, Allowing The Harm To Grow And Rendering Microsoft's Request For Relief Fruitless

If notice is given prior to issuance of a TRO, the botnet will be moved to different domains, on different servers, in different areas, under fictitious names, enabling the parties

controlling the botnet to continue sending billions of spam email and carrying out other conduct causing irreparable injury to Microsoft, its customers and the public. If the botnet domains are allowed to move, the investigation of the botnet and the illicit activities carried out through it would have to be started anew to locate the source of the harm. Providing notice of the requested TRO will undoubtedly facilitate efforts of the parties controlling the botnet to avoid prosecution.

It has long been established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief “fruitless.” *See e.g. In the Matter of Vuitton Et Fils S.A.*, 606 F.2d 1, 4 (2d Cir. 1979) (*per curiam*) (holding that notice prior to issuing TRO was not necessary where notice would “serve only to render fruitless further prosecution of the action”; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, *2 (D. Md. 2010) (granting *ex parte* TRO where “Defendant may dissipate the funds and/or take action to render it difficult to recover the funds ...”) ⁵

Indeed, earlier this year, a federal court issued an *ex parte* TRO suspending internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that “Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff’s] action.” *See FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.) at Dkt. 12, pg. 3 (June 2, 2009 *Ex Parte* Temporary Restraining Order and Order to Show Cause), at Ramsey Decl., Ex. L. Also

⁵ *Crosby v. Petromed, Inc.*, 2009 U.S. Dist. LEXIS 73419, *5 (E.D. Wash. 2009) (granting *ex parte* TRO as “notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...”).

instructive is *Dell, Inc. v. Belgiumdomains, LLC*, 2007 U.S. Dist. Lexis 98676, *4-5 (S.D. Fla. Nov. 21, 2007), where an *ex parte* TRO was issued against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at *4. In *Dell* the Court explicitly found that where, as in the instant case, defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *5-6.

2. If Notice Is Given, Evidence Regarding The Botnet Will Be Destroyed, Disturbing The Status Quo

If notice is given in advance of a TRO, evidence of the botnet will be destroyed. In particular, upon notice, the movement of the botnet domains will not only destroy evidence of the botnet's operation, but will further lead to the loss of evidence available through those domains, such as the identity of infected user computers and other aspects of the system necessary to this litigation. Under such circumstances, courts have issued *ex parte* TROs. See *AT&T Broadband v. Tech Commc'ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Dell, Inc.*, 2007 U.S. Dist. LEXIS 98676 at *4-5; *Little Tor Auto Center v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given").⁶ For this reason, the requested *ex parte* TRO is warranted.

F. Microsoft Will Make Extraordinary Efforts To Provide Notice Of The TRO

⁶ See also *Lorillard Tobacco Co. v. Can-Star (U.S.A.) Inc.*, 2005 U.S. Dist. Lexis 38414, *3-4 (N.D. Ill. 2005) ("an *ex parte* motion to search defendants' residences and seize information concerning their finances is the only manner in which to preserve evidence of the location and extent of their assets..."); *Polo Fashions, Inc. v. Clothes Encounters*, 1984 U.S. Dist. Lexis 18196, *8-9 (N.D. Ill. 1984) (*ex parte* TRO appropriate where evidence "relating to the source and the amounts of such merchandise might disappear and the distributor or source of supply thereof remain undetected ...").

And The Preliminary Injunction Hearing And To Serve The Complaint.

To ensure Due Process, immediately upon entry of the requested *ex parte* TRO, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to the Doe Defendants and to serve the complaint.

Microsoft Will Provide Notice To Doe Defendants By Personal Delivery: Microsoft has identified one Doe Defendant that has provided contact information in Beaverton Oregon. (Ramsey Decl., ¶ 2.v.) Pursuant to Rule 4(e)(2)(A), Microsoft plans to effect formal notice of the preliminary injunction hearing and service of the complaint by hand delivery of the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court. (*Id.*, ¶ 14.) Microsoft has hired a process server who is prepared to immediately attempt service in Oregon. (*Id.*)

Microsoft Will Provide Notice Through The Hague Convention On Service Abroad: Microsoft has also identified twenty-six (26) Doe Defendants that have provided contact information in China. (Ramsey Decl., ¶ 2.a.- 2.u, 2.w – 2.aa.) Pursuant to Rule 4(f)(1), Microsoft is prepared to effect notice of the preliminary injunction hearing and service of the complaint through the Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents ("the Hague Convention"). (*Id.*, ¶ 15.) Microsoft has translated all relevant pleadings into the Chinese language and will immediately request, pursuant to the Hague Convention, that the Chinese Central Authority deliver the summons, Microsoft's Complaint, the instant motion and supporting documents and any Order issued by this Court to Doe Defendants via the contact information provided in China. (*Id.*).

Microsoft anticipates that this means of notice of the preliminary injunction hearing and service of the Complaint could take approximately three (3) to six (6) months to effect service through China's Central Authority. (*Id.*) Accordingly, in addition to making every effort to

expedite this process, given the irreparable harm and the need for prompt relief, Microsoft and its counsel will also provide notice of the TRO and the preliminary injunction hearing and will effect service of the complaint through other means described below.

Microsoft Will Provide Notice By Email, Facsimile And Mail, As Agreed By Doe Defendants In Their Domain Agreements: Microsoft will provide notice of the preliminary injunction hearing and will effect service of the complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses provided by the domain registrants for purposes of resolving disputes regarding the domains. (Ramsey Decl., ¶ 16) When the Doe Defendants registered their domains with the four Chinese domain registrars at issue (Xin Net, eName and China Springboard) and the single U.S. registrar (Wild West Domains), they were required to execute a form registrar-registrant agreement. (*Id.*, Exs. A-D, S) Among other things, these agreements prohibited the abuse at issue in this case and, through the agreements, Doe Defendants agreed that notice of disputes regarding the domains could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provided by them. (*Id.*, Ex. A at p. 1 and §§ 2.1-2.2, 5.1-5.5, 5.11-5.12, 7.5, 8.3; Ex. B at §§ 1, 5-7, 11-12, 14; Ex. C at §§ 2, 6, 9-10; Ex. D at p. 1 and §§ 3, 4, 6-7; Ex. S at §§ 2, 6-11, 18).

Similarly, the registrar-registrant agreements incorporated the dispute resolution policies from the Internet governing body, the Internet Corporation for Assigned Names and Numbers (“ICANN”). (*Id.*) ICANN’s Rules for Uniform Domain Name Dispute Resolution Policy (“Uniform Dispute Resolution Policy”) authorizes service of a complaint regarding domains by mail, facsimile and be e-mail. (Ramsey Decl., ¶¶ 24-37, Exs. H-K) Accordingly, Doe Defendants have agreed to notice by these means and such notice is reasonable, under the circumstances.

Microsoft Will Provide Notice To Doe Defendants By Publication: Microsoft will notify the Doe Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publicly accessible source on the Internet for a period of 3 months. (Ramsey Decl., ¶ 17) Such public notice will be provided on the Internet in English and in Chinese. (*Id.*) Microsoft will also effect notice by additional methods as may be directed by the Court.

G. Microsoft's Proposed Means Of Service Satisfy Due Process.

Notice and service by personal delivery and through the Hague Convention satisfy Due Process. Notice and service by e-mail, facsimile, mail and publication also satisfy Due Process and are necessary under the circumstances. Microsoft hereby formally requests that the Court approve and order the alternative means of service, discussed above.

First, all Doe Defendants have agreed to legal notice by e-mail, facsimile and mail in their registrar-registrant agreements and will expect notice by those means. The agreements specifically authorize registrars to suspend, cancel, transfer or modify domains for breach or if ordered by a Court and to notify Doe Defendants by these means. (Ramsey Decl., Ex. A at p. 1 and §§ 2.1-2.2, 5.1-5.5, 5.11-5.12, 7.5, 8.3; Ex. B at §§ 1, 5-7, 11-12, 14; Ex. C at §§ 2, 6, 9-10; Ex. D at p. 1 and §§ 3, 4, 6-7; Ex. S at §§ 2, 6-11, 18). Accordingly, notice by such means should certainly be sufficient when the same relief is carried out by U.S. Court order. The Supreme Court has recognized that notice by methods consented to in an agreement satisfies Due Process. *Nat'l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311 (1964) ("And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.").

Second, notice by e-mail, facsimile, mail and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of

the TRO, the preliminary injunction hearing and the lawsuit. *See Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).⁷ Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve foreign defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g. FMAC Loan Receivables, v. Dagra*, 228 F.R.D. 531, 535-536 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products North Am., Inc. v. Dagra*, 236 F.R.D. 270, 271-273 (E.D. Va. 2006) (approving notice by publication); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization).

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As was recently observed:

[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is email—the method of communication which [Defendant] utilizes and prefers. In addition, email was the only court-ordered method of service aimed directly and instantly at [Defendant] ... Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, email may be the only means of effecting service of process.

Rio Properties, Inc. v. Rio International Interlink, 284 F.3d 1007, 1014-1015 (9th Cir. 2002).⁸

⁷ Whether such methods are sufficient turns on their “ability to inform people of the pendency of proceedings that affect their interests” in light of “the practical application to the affairs of men as they are ordinarily conducted.” *Greene v. Lindsey*, 456 U.S. 444, 451 (1982); *see also Mullane*, 339 U.S. at 315 (“The means employed must be such as one desirous of actually informing the absentee might reasonably adopt to accomplish.”).

⁸ *Rio Properties* has been followed in the Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (E.D. Va. 2005) (following *Rio*); *BP Prods. N. Am, Inc.*, 232 F.R.D. at 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) (“The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any

Other courts, dealing particularly with service in China have authorized service by facsimile and e-mail as consistent with Rule 4(f)(3) and the Hague Convention. *See MacLean-Fogg Co. v. Ningbo Fastlink Equip. Co. Ltd.*, 2008 U.S. Dist. LEXIS 97241, *4-7 (N.D. Ill. 2008) (“China and the United States are both signatories to the Hague Convention. The Hague Convention does not prohibit service by e-mail or facsimile.”).⁹ In this case, the evidence suggests that e-mail addresses provided by domain registrants is likely to be the most accurate and viable contact information. (Ramsey Decl., ¶¶ 3-8) Moreover, if the physical address information provided by Doe Defendants to the domain registrars turns out to be false and Doe Defendants’ whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as e-mail and publication, would be appropriate for that reason as well. *See BP Products North Am., Inc.*, 236 F.R.D. at 271 (“The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.”)

For all of the foregoing reasons, Microsoft respectfully requests that the Court enter the requested TRO and order to show cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3), satisfy Due Process and are reasonably calculated to notify defendants of this action. *See e.g. AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, *3 (D. Md. 2010) (granting *ex parte* TRO and ordering prompt “notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services.”)

IV. CONCLUSION

controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.* ...)

⁹ *See also Williams-Sonoma, Inc. v. Friendfinder, Inc.*, 2007 U.S. Dist. LEXIS 31299, *5-6 (N.D. Cal. 2007) (service by email consistent with Hague Convention and warranted in case involving misuse of Internet technology by international defendants).

For the reasons set forth herein, Microsoft respectfully requests that this Honorable Court grant its motion for a TRO and order to show cause regarding a preliminary injunction, directing that (1) resolution of the 273 domains used to control the Waledac botnet be immediately suspended at the registry (Verisign) administering the top-level domain and at the registrars and (2) the domains be placed into escrow with Verisign, pending a resolution of the issues. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

Dated: February 22, 2010.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP



PRESTON BURTON (Va. State Bar No. 30221)
REBECCA L. MROZ (Va. State Bar No. 77114)
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
pburton@orrick.com
bmroz@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)
JACOB M. HEATH (*pro hac vice* application pending)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com

Attorneys for Plaintiff Microsoft Corp.